

ISB IT Portfolio Policy Compliance Handbook for Small Agencies



SMALL AGENCY CLIENT SERVICES

Providing small governmental clients
with objective advice for effective information
technology planning and investment decisions

Prepared by Small Agency Client Services



ISB IT Portfolio Policy Compliance Handbook for Small Agencies

Purpose:

Management personnel of small state agencies are often challenged by limited information technology (IT) support staff and small investments in IT. These managers can use Information Services Board (ISB) policies and standards for IT Portfolio management to better manage their technology investments. Since we have created these policies and standards in consideration of the complex IT investments of large agencies, small agency managers may have difficulty interpreting and applying them. We have developed this handbook to help small agency managers comply with ISB requirements for planning, getting approval, reporting on, and securing their IT investments.

You can meet both the letter of the law and the intent of the ISB requirements with thoughtful reflection and brief reporting by using this handbook as a guide. Our intent is not to minimize the value of the reporting, but to provide you with tools to evaluate your IT investments and identify areas needing attention. We have suggested formats to help you organize your thoughts, analyze your IT investments' alignment with your needs and efficiently report the required information.

When planning your IT investments, consider the requirements that are defined in ISB policies. Your IT investments must:

- meet agency business needs.
- provide for efficient and compatible internal systems.
- secure valuable data and assure timely recovery from disruption.
- work with statewide systems like human resources, accounting and purchasing.
- leverage opportunities to share IT services using the capacity of DIS and other agencies.

You must document and update these considerations yearly in your agency IT Portfolio. You may also need to develop IT Investment Plans prior to making individual investments. You are also required to develop specialized plans for security and disaster recovery. You can use the IT Portfolio to tie all of your planning together.



Scope:

In this Handbook, you will find annual reporting requirement guides for these four areas:

- IT Portfolio Policy and Standard (100-P1, 101-S1)
- IT Security Policy and Standard (400-P1, 401-S1)
- IT Disaster Recovery/Business Resumption Policy and Standard (500-P1, 501-S1)
- IT Investment Policy and Standard (for individual IT investments) (200-P1, 201-S1)

See <http://www.dis.wa.gov/portfolio/index.htm> for copies of these policies.

Approach:

For each annual reporting requirement, you will find:

- basic requirements.
- questions to identify the information needed to achieve compliance (note that nearly all content is guided by questions to simplify submission and maintenance of this important document).
- “Suggested Formats” or “Required Formats” to help you organize information.
- “Tips” to guide your consideration of how your agency meets the intent of ISB policies and standards.

We have also included a sample, fictional small agency report in The Sample IT Portfolio.

Look for these icons to (link) to a format, tip, or example:



Required Format



Suggested Format



Tip



Example



Annual Reporting Requirements:

By using this handbook, you will be able to do what's required to meet your annual reporting requirements. Once you're done, complete the following steps by August 31 of each year:

- Your agency Director must complete a verification memo addressed to the DIS MOSTD Deputy Director with a copy to your DIS MOSTD Consultant that includes:
 - 1) verification that you have followed IT Portfolio policies and standards in planning for your IT investments.
 - 2) verification that you have followed IT Portfolio policies and standards for Security and Disaster Recovery/Business Resumption.
 - 3) verification that you have entered the information from Section 3 of the IT Portfolio into ePortfolio.
 - 4) verification that you have delivered the IT Portfolio to DIS MOSTD.

Submit your IT Portfolio document(s) to DIS MOSTD by e-mailing electronic copies (Word or PDF) or by posting the IT Portfolio to your Intranet and giving your DIS MOSTD Consultant the URL.



Example

See an example of the annual verification letter in the Donut Commission Sample IT Portfolio, page 32.



IT Portfolio Policy and Standard Basic Compliance Reporting:

The IT Portfolio is a collection of documents that you need to fulfill your reporting requirements. It includes your overall plans, your current IT resource inventory and budget, and current and planned projects. Your completed IT Portfolio will include six sections. Following is the outline for the information required in the IT Portfolio:

Section 1 – Agency Portfolio Overview

- A. Purpose of the IT Portfolio
- B. Convergence of Business Mission and IT Vision
- C. IT Plans, Proposals, and Acquisitions Process
- D. Overview of IT Infrastructure
- E. Analysis of IT Infrastructure
- F. Challenges, Opportunities and Solutions
- G. Prioritization Process

Section 2 – Agency Strategic Business Plan (link to existing strategic business plan)

Section 3 – Agency Technology Infrastructure (inventory of current investments)

- A. Current and Projected IT Budget
- B. IT Personnel
- C. Personal and Workgroup Computing
- D. Geographic Information Systems
- E. Security and Disaster Recovery/Business Resumption Plans
- F. Public Access
- G. Application Systems and Databases

Section 4 – Technology Investment/Project Summaries (current)

Section 5 – Technology Investment/Project Summaries (planned)

Section 6 – Annual Technology Investment and Project Reviews (assessment of results)

You will also need to prepare your Security Plans, Disaster Recovery Plans, and individual IT Investment Plans, which you must reference in your IT Portfolio. Although we haven't provided detailed guidance to help you complete these plans, we have provided some tips on page 24, Appendix A -- Checklist for Security and Disaster Recovery/Business Resumption (DR/BR) Planning for Small Agencies.

Section 1 – Agency Portfolio Overview

The Agency Portfolio Overview is an “executive summary” of your IT investments and how they support your agency’s mission. You will provide greater detail about your IT investments in the next five sections. Complete those sections first, and then write this section with reference to the details in your completed forms.

When you are ready to complete this section, respond to the following eight topics:

A. Purpose of the IT Portfolio

1. How will your IT Portfolio planning support your agency?



Example

See an example of a brief opening paragraph in the Donut Commission Sample IT Portfolio, page 3.

B. Convergence of Business Mission and IT Vision – Use your agency’s Strategic Business Plan to complete this section (see Section 2).

1. See Figure 1 below for a Suggested Format for this subsection.
2. Briefly describe the background, scope, funding, and composition of your agency.
3. What is your agency mission, and vision for carrying it out in the next few years?
4. What are the primary services that your agency delivers?



Tip

Describe these at a high level and match the description to your organizational structure.

5. How do your current IT investments contribute to achieving your mission and delivering your services?



Tip

This is one of the subsections that you will detail in section 3. Complete this subsection after you have finished Section 3.



Example

See an example of a Convergence of Business Mission and IT Vision in the Donut Commission Sample IT Portfolio, page 4.



Figure 1 – Business Mission/IT Current Capabilities Convergence Table



Suggested Format

Business Needs	Current IT Contributions
Our Mission and Vision are...	In general, our IT investments and resources help us achieve our mission by...
Our primary services are...	Our IT investments and resources directly support service delivery by...



Example

See the Donut Commission Sample IT Portfolio, pages 5-6, for an example of this Suggested Format.

C. IT Plans, Proposals, and Acquisitions Process

1. How does your agency plan for IT acquisitions and how is this process integrated with budgeting for the business of your agency?
2. How do you make sure that you follow state standards when you select and acquire IT resources?



Example

See an example of this subsection in the Donut Commission Sample IT Portfolio, page 7.

D. Overview of IT Infrastructure

1. See Figure 2 below for a Suggested Format for this subsection.
2. Your workstations, networks, servers, software, and data – this subsection is an overview – Sections 3 and 4 contain more details
3. Include a diagram of your network, facilities, servers, and workstations if one is readily available.



Example

See the Donut Commission Sample IT Portfolio, page 34, for an example diagram.

Figure 2 – Overview of IT Infrastructure Table



Suggested Format

Infrastructure Requirements or Components	Current Status and Capabilities
The number of agency users supported by the IT infrastructure is:	Describe...
The type and number of external customers supported by the IT infrastructure is:	Describe...
The IT support comes from:	Describe...
Our workstations include:	Describe...
Our servers include:	Describe...
Our network components include:	Describe...
Specialized infrastructure for security and disaster recovery includes:	Describe...
Critical application software and databases include:	Describe...



Example

See the Donut Commission Sample IT Portfolio, page 8, for an example of this Suggested Format.



E. Analysis of IT Infrastructure Spending

1. How do your actual expenditures on IT break down by type of expenditure for the previous fiscal year?



Tip

This assumes that you will be completing this analysis at the end of the fiscal year, but you may complete this table for the 12-month period that has just passed.

2. How do your projected expenditures on IT break down by type of expenditure for the current fiscal year?
3. Use the categories from Section 3A and create a pie chart, or see Figure 3 below for a Suggested Format for this subsection.

Figure 3 – Analysis of IT Infrastructure Spending Table



Suggested Format

IT Spending Category	Previous Yr. Actual	% of Total	Current Year Projected	% of Total
Hardware purchase or lease:				
Software purchase or lease:				
Hardware repairs and maintenance:				
Software enhancements and maintenance:				
Telecommunications and networking:				
Data processing services (e.g. DIS services):				
IT FTE salary and benefits:				
Personal or purchased contractor services:				
IT Training:				
Totals		100%		100%



Example

See the Donut Commission Sample IT Portfolio, page 10, for an example of this Suggested Format.

F. Challenges, Opportunities, and Solutions

In this subsection, you will describe your current and planned IT investments that will help you achieve the business objectives of your agency. Your descriptions may be very brief or extensive, depending on current projects and future plans. Use Sections 4 and 5 of the IT Portfolio as a reference for this section.

1. In general, how do you hope to use IT investments to achieve your agency business mission, objectives, and services?
2. What opportunities do you see to collaborate with other state agencies and to contribute to the state IT plan?



Example

See the Donut Commission Sample IT Portfolio, page 11, for an example of this Suggested Format.

3. What specific agency business objectives will you be supporting with current or future IT investments in the next biennium? See Figure 4 below for a Suggested Format for this information.

Figure 4 – Current and Future IT Investments to Meet Business Objectives



Suggested Format

Business Objective	Current or Planned IT Investment	Impact on IT Infrastructure
Our objectives for the coming biennium and beyond are...	We are achieving these objectives by making the following current and planned IT investments and resources:	High, Medium, or Low (considering new resources, funds, process change, or effort required)



Example

See the Donut Commission Sample IT Portfolio, page 12, for an example of this Suggested Format.



G. Prioritization Process

1. What are your current IT investment priorities?
2. What is your process for prioritizing IT resources?
3. How do you consider hardware and software obsolescence in your IT investment prioritization?



Tip

Work toward a plan for continuous maintenance and upgrade of your hardware and software to avoid having to replace a lot at once.



Example

See an example of Section 3, Agency Technology Infrastructure (inventory) in the Donut Commission Sample IT Portfolio, pages 15-24.

Section 2 – Agency Strategic Business Plan (link to existing strategic business plan)

- A. Attach or create a link to your agency Strategic Business Plan.

Section 3 – Agency Technology Infrastructure (Inventory)

The Agency Technology Infrastructure is your description of existing IT investments within your agency. This set of questions, taken directly from the IT Portfolio Standard, is an inventory of your technology and supporting staff investments.



Example

See an example of this subsection in the Donut Commission Sample IT Portfolio, page 13.



Tip

You will also submit subsections A through D of Section 3 in your IT Portfolio document, and on a Web site – ePortfolio – for automatic reporting to DIS. Contact your MOSTD consultant for instructions to e-portfolio.

Include all IT expenditures, not just those in the IT budget. For a small agency, we recommend that you complete this update at the end of each fiscal year or 12-month period that has just passed. For all of the tables in this section, enter actual expenditures from the fiscal year or 12-month period that has just passed, and projected costs for the beginning of the next fiscal year or 12-month period. Indicate the fiscal year or 12-month period in the first column.



Required Format

A. Current and Projected IT Budget for the entire agency

Reporting Period	Total Agency IT Budget*	Hardware Purchase and/or Lease	Software Purchase and/or Lease	H/W Repairs and Maintenance	S/W Enhancements and Maintenance
Indicate Current Fiscal Year	(Projected)	(Projected)	(Projected)	(Projected)	(Projected)
Indicate Current Fiscal Year	(Actuals)	(Actuals)	(Actuals)	(Actuals)	(Actuals)
Indicate Next Fiscal Year	(Projected)	(Projected)	(Projected)	(Projected)	(Projected)

* Total IT budget includes amounts from both this section (A.) and the next section (B.)

Reporting Period	Telecommunications	Data Processing Services (e.g. DIS services)	If applicable, list and identify other major IT expenses here
Indicate Current Fiscal Year	(Projected)	(Projected)	(Projected)
Indicated Current Fiscal Year	(Actuals)	(Actuals)	(Actuals)
Indicated Next Fiscal Year	(Projected)	(Projected)	(Projected)



B. IT Personnel

Reporting Period	Total Agency IT FTEs (include WMS positions)	Salaries and Benefits	Personal and Purchased Services	Professional Development of IT Staff
Indicate Current Fiscal Year	(Projected)	(Projected)	(Projected)	(Projected)
Indicate Current Fiscal Year	(Actuals)	(Actuals)	(Actuals)	(Actuals)
Next Fiscal Year	(Projected)	(Projected)	(Projected)	(Projected)

C. Personal and Workgroup Computing

Personal Computers				
1.Total Agency FTEs	2.Total number of PCs (exclude servers)	3.Planned number of PC replacements next fiscal year	4.Agency intended refresh cycle in months	5.PCs donated to schools in last 12 months


Personal Computers:

1. What is the total agency FTE count for the current fiscal year?
2. How many personal computers (PCs) does the agency currently have (excluding servers)?
3. How many of these PCs does the agency plan on replacing in the next fiscal year?
4. If your agency has an established PC refresh cycle, what is the length of that cycle?
5. If your agency donates used PCs to schools, approximately how many did you donate in the past 12 months?

Servers			
6.Total number of servers	7.Number of servers to be replaced next fiscal year	8.Number of servers planned to be added in next fiscal year	9.Factors driving server acquisition strategy

Servers:

6. How many servers does your agency currently lease or own?
7. How many of these current servers do you plan on replacing during the next fiscal year?
8. How many additional servers do you plan to purchase or lease during the next fiscal year?
9. Which of the following are driving your server acquisition strategy? (pick one or more)
 - server consolidation
 - increased application utilization
 - new application deployment
 - disaster recovery/redundancy
 - other



Network Connectivity	
10. Percentage of agency staff with Inside Washington (intranet) access	11. Agency primary network operating system

Networks:

10. What percent of agency staff have access to the state intranet portal (Inside Washington)?
11. What is the primary network operating system within our agency?

Desktop Office Suite	
12. Primary desktop office product suite	13. If not XML enabled do you plan to be within 12 months? (yes/no)

Desktop Office Suite:

12. What office product suite does your agency use as its primary desktop tool?
13. If desktop office suite is not XML enabled, do you plan to migrate to a version that is within the coming biennium? (yes/no)

D. Geographic Information Systems

GIS Category Descriptions:

Many agencies have a significant investment in GIS technology or rely on the technology to meet mission critical information requirements. If your agency uses GIS in this context, please respond to the following.

1. GIS Staffing (FTEs) - (Please indicate if these FTEs are reflected in Section 3.B.1 "Total Agency IT FTEs")
 - centralized support - indicate FTEs currently devoted to a corporate or centralized GIS support effort.
 - program area support - indicate FTEs currently attached to program areas for GIS support.
2. Software - identify GIS software packages and number of licenses currently maintained for each.
3. Hardware - identify hardware platforms used to support GIS.
4. Major applications - identify and provide brief description of major/mission critical GIS applications.
5. GIS Database Environment - identify vendor databases (e.g. ARC SDE, Oracle, etc.) used to support mission critical GIS effort and indicate number of GIS applications supported by each database.
6. Critical GIS Datasets - identify GIS datasets that are critical to support of your agency mission.



Indicate the fiscal year being reported: FY_____

	1. Number of GIS Staff (FTEs)	Indicate here if included in 3.B.1 "Total Agency IT FTEs"
Central Support		(yes/no)
Program Area Support		(yes/no)
	2. GIS Software	
Vendor Name		
Product Name		
Number of Licenses		
	3. Hardware	
Make/Model		
How Many		
Is this equipment included in Section 3C.2 "Total Number of PCs?"	(yes/no)	
Is this equipment included in Section 3C.6 "Total Number of Servers?"	(yes/no)	
	4. Major GIS Application(s)	
Application Name / Description		

	5. GIS Database(s) Environment	
Vendor Name		
Number of applications		
	6. Critical GIS Datasets	
Name(s)		

E. Security and Disaster Recovery Resumption Plans

Every agency is required to comply with ISB policies for IT Security and IT Disaster Recovery and Business Resumption Planning.

1. Describe your actions to review and approve the agency security and disaster recovery/business resumption processes including updates and tests in the past year.



Tip

Although we haven't provided a complete guide to help you develop appropriate plans for security or Disaster Recovery/Business Resumption, we have provided checklists in Appendix A of this handbook.

Use the checklists to assess whether your agency has adequately followed the ISB policies and standards. Contact DIS SACS for guidance and resources to make necessary security and Disaster Recovery/Business Resumption plan improvements.



Example

See an example of security compliance using the Donut Commission Sample IT Portfolio, page 18.



Example

See an example of Disaster Recovery/Business Resumption compliance using the Donut Commission Sample IT Portfolio, page 21.



Tip

The plans and actions that enable compliance with these policies are not part of the IT Portfolio. You are required to submit an annual verification letter with your annual submission of updates to the IT Portfolio. You can complete the annual verifications as a single letter, along with verification from your agency Director that within your agency, the IT Portfolio requirements have been met.



Example

See an example of a verification letter in the Donut Commission Sample IT Portfolio, page 32.



F. Public Access

You must work with existing resources to provide electronic access and two-way interaction with agencies' information (RCW 43.105.270). This includes access that overcomes barriers caused by separation of agency responsibilities to meet individual or business needs, office hours, and accessibility challenges for the handicapped. The RCW applies to information only requests, and to forms and transactions that agencies may require of customers for their services.

1. Describe your progress toward meeting the requirements of RCW 43.105.270.



Suggested Format

See Figure 5 below for a Suggested Format for this subsection.

Figure 5 – Public Access Information

Public Access Questions	Capabilities and Initiatives
What are the general content and capabilities of the agency's Web site?	Describe...
What transactions or information collection requirements are available through electronic access?	Describe...
What are your agency's future plans to improve electronic public access?	Describe...



Example

See an example of this subsection in the Donut Commission Sample IT Portfolio, page 22.

G. Application Systems and Databases

In this subsection, you will inventory your mission critical applications and databases. You may have few or no applications or databases that meet the ISB policy definition of mission critical. By definition, these are systems for which short term loss of capability could significantly impact:

- the health or safety of the public or state workers
 - income maintenance for citizens or government employees
 - payments to vendors for goods or services
 - the legal or fiscal integrity of state operations
1. List any mission critical applications in use by your agency.
 2. Complete the following information for applications and databases that are very important to meeting your business objectives.



Tip

While your agency may not have applications that are deemed critical by ISB policy, you may have agency applications that are critical to your mission. You are encouraged to document these in the suggested format to bring attention to the important data and functions supported by your agency's systems.



Suggested Format

See Figure 6 below for a Suggested Format for this subsection.

Figure 6 – Applications and Databases

Name, year implemented, brief description, future prospects	Types and numbers of users	Functions and transactions automated, interfaces to other systems	Nature of the information stored by this application or database	Hardware and software in use
Describe...	Describe...	Describe...	Describe...	Describe...



Example

See an example of this subsection in the Donut Commission Sample IT Portfolio, pages 23-24.



Section 4 – Technology Investment/Project Summaries (current)

The Technology Investment/Project Summary is your detailed description of the current and planned projects to implement your technology investments. By applying effective project management – good definition and management of scope, schedule, resources, acquisitions, risks, quality, and communications – you will be able to achieve project success and comply with ISB policy (IT Project Management Policy 300-P1). You must provide information in this section for each investment. You can reference your IT Investment Plans* (if required) and other project planning.



Tip

*Information about IT Investment Plans can be found in ISB Policy 200-P1 and Standard 201-S1. Contact your DIS MOSTD consultant for help on completing IT Investment Plans.



Suggested Format

For each current project, complete the required information included in the format below (Figure 7):

Figure 7 – Technology Investment/Project Summaries

Investment Project Name:

Brief Description and Scope of Functionality	Business Objectives Supported, Benefits Expected	Impacts on the Organization, Others, and IT Infrastructure	Risks
Describe...	Describe...	Describe...	Describe...

Cost Estimate	Agency FTEs and Vendor Support Needed	Schedule	Executive Sponsor and Project Manager Contacts
Describe...	Describe...	Describe...	Describe...

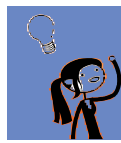


Example

See an example of this Suggested Format in the Donut Commission Sample IT Portfolio, pages 26-27.

Section 5 – Technology Investment/Project Summaries (planned)

The Technology Investment/Project Summaries are your detailed descriptions of your current and planned projects that will implement your technology investments. By applying effective project management – good definition and management of scope, schedule, resources, acquisitions, risks, quality, and communications – you will be able to achieve project success and comply with ISB policy (IT Project Management Policy 300-P1). You must provide information in this section for each investment. You can reference your IT Investment Plans* (if required) and other project planning.



Tip

* Information about IT Investment Plans can be found in ISB Policy 200-P1 and Standard 201-S1. Contact your DIS MOSTD consultant for help on completing IT Investment Plans.



Suggested Format

For each current project, complete the required information included in the format below (Figure 7a):

Figure 7a: Technology Investment/Project Summaries

Investment Project Name:

Brief Description and Scope of Functionality	Business Objectives Supported, Benefits Expected	Impacts on the Organization, Others, and IT Infrastructure	Risks
Describe...	Describe...	Describe...	Describe...

Cost Estimate	Agency FTEs and Vendor Support Needed	Schedule	Executive Sponsor and Project Manager Contacts
Describe...	Describe...	Describe...	Describe...



Example

See an example of this subsection in the Donut Commission Sample IT Portfolio, pages 26-27.



Section 6 – Annual Technology Investment and Project Reviews (assessment of results)

The Annual Technology Investment and Project Review is verification that your agency has completed an annual review of all IT investments, and has reviewed your ongoing Oversight Level 2 or 3 IT investment projects.

Although this section typically includes project reviews for ISB Severity and Risk Matrix level 2 or 3 projects, you may not have any projects at this level to review. If you do have level 2 or 3 projects to review, we have outlined the following questions to help you meet reporting requirements.

1. List any Oversight Level 2 and 3 projects currently underway or completed since your last annual submission of the IT Portfolio.
2. For each project, answer the following questions:
 - a. How timely was project delivery compared to the original schedule? How did you manage variances and what were the impacts?
 - b. What was the cost of project delivery compared to the original budget? How did you manage variances and what were the impacts?
 - c. What functionality was delivered compared to original expectations. How did you manage variances and what were the impacts?
 - d. What benefits were expected? What changes in expectations have occurred?



Suggested Format

See Figure 8 below for a Suggested Format for this subsection.

Figure 8 – Annual Assessment of IT Investment Results (repeat for each project)

Name of Project	Results
How timely was project delivery compared to the original schedule? How were variances managed and what were the impacts?	Describe...
What was the cost of project delivery compared to the original budget? How were variances managed and what were the impacts?	Describe...
What functionality was delivered compared to original expectations. How were variances managed and what were the impacts?	Describe...
What benefits were expected? What changes in expectations have occurred?	Describe...




Example

See an example of this subsection in the Donut Commission Sample IT Portfolio, pages 28-29.



Tip

A diagram can help describe your project results. See an example diagram on page 31 of the Donut Commission sample.



By August 31 of each year, you must mail to the DIS Deputy Director of MOSTD and include in this section, a single verification letter. Include in the letter your agency Director's certification of compliance with IT Portfolio, Security, and Disaster Recovery/Business Resumption policies and standards.



Example

See an example of the annual verification letter in the Donut Commission Sample IT Portfolio, page 32.



Appendix A – Checklists for Security and Disaster Recovery/Business Resumption (DR/BR) Planning for Small Agencies

General Guidance:

You must make sure that the size and complexity of your agency security program corresponds with that of your agency's IT systems. You must also make sure that your exposure to risk is in compliance with ISB standards for security and DR/BR. For small agencies, both of these factors should be small, so the IT Security and DR/BR plans and practices can be brief and practical. This appendix includes a set of questions that can serve as a checklist for agency management in evaluating their security and DR/BR plans. Agency management, agency IT management, and service providers – supporting agencies, DIS, and vendors – can use these checklists when examining whether the agency has covered requirements for security and DR/BR measures. Completing these checklists will help you make sure your agency has met the ISB standards, and will help substantiate that your management is responsive to and accountable on these important requirements. By providing brief summary responses to the checklist, you can support the annual verification letters.



Example

See an example of this security checklist in the Donut Commission Sample IT Portfolio, page 18.

Security Checklist:

Management Question:	Responses (Summary level – see the agency's IT Security Plan for details)
What policies and plans does the agency have to guide its employees in assuring the security of the agency's IT assets and data?	Summary description...
What IT capabilities does the agency share with other agencies and the state as a whole? How do they support the agency's IT asset security?	Summary description...
How do the agency's security plans address the agency's reliance on others and the impact of the agency's practices on the state IT infrastructure as a whole?	Summary description...
Who has supported development of the agency's security plans and do they have the appropriate training and experience?	Summary description...
How has the plan been tested, updated, and audited in the past year to assure effectiveness, currency, and compliance? (Independent audits are required every three years.)	Summary description...



Management Question:	Responses (Summary level – see the agency's IT Security Plan for details)
How is sensitive information in the security plan protected from unauthorized access?	Summary description...
What does the agency do to assure its personnel and contract resources understand and follow the agency's security plan?	Summary description...
How has the agency assessed its IT assets, impacts of security failure, and threats and risks posed by security failures?	Summary description...
How are the agency's physical facilities and IT assets safeguarded?	Summary description...
How has the agency identified and protected its important data from compromise or unauthorized use?	Summary description...
How does the agency use data encryption?	Summary description...
How has the agency assured that its important data and application program code are backed up, secure, and restorable?	Summary description...
How does the agency protect from infection by viruses and similar threats?	Summary description...
How does the agency secure its networks from unauthorized access?	Summary description...
How does the agency maintain currency of network and virus protection software?	Summary description...
How does the agency assure effective and appropriate use of Web browsers and e-mail?	Summary description...
How does the agency secure remote access to its applications and information?	Summary description...
How does the agency assure compliance with use of strong passwords per ISB security policy?	Summary description...
How does the agency identify and authenticate users of its data and applications on the network or via the Internet?	Summary description...
Has the agency identified applications that execute agency transactions that are accessible via the Internet and assured DIS review and approval?	Summary description...



Example

See an example of the DR/BR checklist in the Donut Commission Sample IT Portfolio, page 21.

DR/BR Checklist:

Management Question:	Responses (Summary level – see the agency's IT Security Plan for details)
How has the agency assessed its IT assets, impacts of disasters or disruptions, and threats and risks posed that should be mitigated?	Summary description...
How has the agency identified and prioritized its mission critical and important services that must be recovered from disruption?	Summary description...
How has the agency prepared DR/BR plans that meet the state standards?	Summary description...
How does the agency collaborate with supporting agencies to create complete and appropriate DR/BR capabilities?	Summary description...
Who has supported development of the agency's DR/BR plans and do they have the appropriate training and experience?	Summary description...
How has the plan been tested, updated, and audited in the past year to assure effectiveness, currency, and compliance? (Independent audits may be done by the State Auditor.)	Summary description...
What are the agency's primary recovery requirements (what has to be put back in operations first) and what are the primary means to assure that this can happen?	Summary description...
What alternate facilities, IT, and communications capabilities would be utilized to recover from a disaster?	Summary description...
How is data backed up, safeguarded, and tested to assure that it can be recovered appropriately?	Summary description...
How does the agency organize its people to respond, contact first responders, and take steps to reduce the severity of the impacts?	Summary description...



Overview of Security References:

We have derived the following table from the ISB IT Security Standards, 401-S2, P. 19 to provide an overview of the IT Security requirements and references.

Policy	Relevant Standard Section
1. Each agency must operate in a manner consistent with the maintenance of a shared, trusted environment	Standards for IT Security Program Development and Maintenance (Section I) Network Security Standards (Section II, D)
2. Each agency must establish its networks and secure applications within the Washington State Digital Government Framework. This requires that all parties interact with agencies through a common security architecture and authentication process	Network Security Standards (Section II, D) Access Security Standards (Section II, E)
3. Each agency that operates its applications and networks within the Washington State Digital Government Framework must subscribe to the principles of shared security	Standards for IT Security Program Development and Maintenance (Section I) Network Security Standards (Section II, D) Access Security Standards (Section II, E)
4. Each agency must address the effect of using the Internet to conduct transactions for state business with other public entities, citizens and businesses	Network Security Standards (Section II, D) Access Security Standards (Section II, E)
5. Each agency must ensure staff is appropriately trained in IT security procedures	Personnel Security Standards (Section II, A)
6. Each agency must review its IT security processes, procedures, and practices at least annually and make appropriate updates after any significant change to its business, computing or telecommunications environment	Standards for IT Security Program Development and Maintenance (Section I)



Policy	Relevant Standard Section
7. Each agency must conduct an IT Security Policy and Standards Compliance Audit once every three years. It must be performed by parties independent of the agency's IT organization	Standards for IT Security Program Development and Maintenance (Section I)
8. Pursuant to RCW 43.105.017(3), agency heads will confirm in writing that the agency is in compliance with this policy	Standards for IT Security Program Development and Maintenance (Section I)
9. The State Auditor may audit agency IT security processes, procedures and practices	Standards for IT Security Program Development and Maintenance (Section I)

You can find DR/BR Standards in 501-S1 and a helpful guide for preparing a DR/BR plan in 502-G1.